TOURO COLLEGE
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 36 | Number 2 Article 10

2020

Trimming the Fat: The GDPR as a Model for Cleaning up Our Data Usage

Kassandra Polanco
Touro Law Center

TRIMMING THE FAT: THE GDPR AS A MODEL FOR CLEANING UP OUR DATA USAGE

*Kassandra Polanco**

I. INTRODUCTION

It is not uncommon for someone searching for a new pair of shoes to come across an advertisement for that same pair a few hours later. The average online shopper can understand this basic level of data collection. As valuable as that data is, consumers fail to recognize the extent to which companies track, store, sell, and even lose their data. Some companies are scanning crowds at popular concerts and collecting facial recognition data, while others are recording the way a user holds a cell phone or scrolls through a website.[1]

In the digital age, data collection is a commodity for any company that wants a glimpse into the mind of its consumers. In 2018, the Interactive Advertising Bureau estimated that U.S. companies spent over nineteen billion dollars acquiring and analyzing personal data.[2] Some services, such as Instagram or YouTube, can provide free services to customers because they rely on the collection of personal data for profit.[3] Google, which owns YouTube, is another free service

* I would like to thank the Touro Law Review for their patience and guidance in helping me achieve this accomplishment. I thank my parents and family for their continued support, without which I would not be the woman I am today. I dedicate this piece to all of the inspirational women in my life, inside and out of the legal profession, who motivated me to recognize my responsibility to speak, to write, to learn, and to listen. Touro College Jacob D. Fuchsberg Law Center, J.D. 2020; Arcadia University, B.A. Criminal Justice 2016.

[1] Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED MAGAZINE, (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/.

[2] The Interactive Advertising Bureau Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data & Data-Use Solutions in 2018, Up 17.5% From 017*, IAB (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[3] Matsakis*, supra* note 1.

that collects a staggering amount of data from its users.[4] The data collected from consumers range from social media posts and location data to the unique way they tap and fumble with a smartphone.[5] Companies are tracking and collecting this data through a process known as data mining. Through data mining, companies can discover patterns by combing through large volumes of data.[6] Mass data mining has become the norm, but it comes with a whole new set of issues.

First, many consumers do not have any idea when or how their data is being collected, no less for what it is being used. Data brokers[7] profit from data by creating and selling lists of consumers who share common interests, such as new parents or pet owners.[8] Other businesses[9] have created and sold consumer lists based on different health conditions like anorexia, substance abuse, and depression.[10] Second, unfettered access to data is not necessarily good for businesses. In addition to the possible negative effects on consumers, businesses can become subject to data hoarding. They collect mass quantities of personal data, likely hoping that the value will be discovered later down the line. Last, the increased value of personal data has come to mean quantity over quality. This has led to a data hoarding culture that puts consumers' personal data at an increased risk of data breaches.

Unfortunately, the safety measures the United States (hereinafter "U.S") has in place to regulate big data are not sufficient to protect the personal data of U.S. citizens. Gemalto, a leading global provider of digital security solutions, reported that worldwide, in just the first half of 2018, there were nine-hundred-and-forty-four recorded

---

[4] Dale Smith, *Google Keeps a Frightening Amount of Data on You. Here's How to Find and Delete It,* CNET (Mar. 7, 2020, 4:00 AM), https://www.cnet.com/how-to/google-keeps-a-frightening-amount-of-data-on-you-heres-how-to-find-and-delete-it/.

[5] Matsakis*, supra* note 1.

[6] *Data Mining*, BRITANNICA, https://www.britannica.com/technology/data-mining (last visited May 7, 2020).

[7] Companies that collect information from public records, online activity, and search history resell that information to other companies.

[8] WebFX Team, *What Are Data Brokers – And What Is Your Data Worth? [Infographic]*, WEBFX, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ (last updated Mar. 16, 2020).

[9] The words organization, business, and company will be used interchangeably throughout this Note.

[10] Kashmir Hill, *Data Broker Was Selling Lists of Rape Victims, Alcoholics and 'Erectile Dysfunction Sufferers'*, FORBES (Dec. 19, 2013, 3:40 PM), https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/#4c03b0af1d53.

data breaches.[11] As a result of these breaches, over three billion records were compromised.[12] Of those, the U.S. saw one-thousand-two-hundred-and-forty-four data breaches in 2018, with just over four-hundred-forty-six-million exposed records.[13]

Lawmakers are not taking data breaches seriously enough. Politicians must gain an understanding of how many companies rely on big data to operate. Without a basic understanding of how the world operates in the digital age, Congress is lagging when it comes to protecting U.S. citizens' private information. This is evident through some of the questioning posed by the House Judiciary Committee to Google CEO and Chairman Sundar Pichai in late 2018 or the questions asked to Facebook CEO Mark Zuckerberg earlier that year.[14] This lack of understanding bleeds into many consumers' laissez-faire attitude about their data.

While every state currently maintains data breach legislation, the U.S. lacks legal harmony when it comes to data privacy laws.[15] Mainly, regulations on data privacy are state-specific, but there are some federal laws specific to certain industries, such as healthcare or financial institutions.[16] Federal law in the area of data protection is limited, and there is no federal statute that explicitly guides businesses that interact with citizens of different states, or that operate out of multiple locations.[17] Instead, it is up to individual businesses to sift

---

[11] Breach Level Index, *Data Privacy and New Regulations Take Center Stage: 2018 First Half Review*, GEMALTO, https://www.key4biz.it/wp-content/uploads/2018/10/breach-level-index-report-h1-2018.pdf (last visited Sept. 18, 2019).

[12] *Id.* at 4.

[13] Rob Sobers, *107 Must-Know Data Breach Statistics for 2020*, VARONIS, https://www.varonis.com/blog/data-breach-statistics/#:~:text=The%20United%20States%20saw%201%2C244,stability%20(World%20Economic%20Forum)., (last visited, Jun. 25, 2020).

[14] Conor Cawley, *The Best (and Worst) Questions Congress Asked Google*, TECH.CO (Dec. 11, 2018, 5:46 PM), https://tech.co/news/best-worst-questions-congress-google-2018-12. "Right now, if you google the word 'idiot' under images, a picture of Donald Trump comes up. I just did that. How would that happen?" *Id.*

Minda Zatlin, *The 9 Weirdest and Most Hilarious Questions Congress Asked Mark Zuckerberg*, INC. (Apr. 12, 2018), https://www.inc.com/minda-zetlin/mark-zuckerberg-congress-hearings-funny-stupid-questions.html. For example, "Is Twitter the same as what you do?"; "[i]f I'm emailing within WhatsApp . . . does that inform your advertisers?" *Id.*

[15] Jana N. Sloane, *Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation*, 12 J. MARSHALL L.J. 23, 24 (2018-2019).

[16] *Id.*

[17] *Id.*

through a patchwork of state data breach laws to ensure compliance.[18] This lack of uniformity can easily become complicated and unnecessarily costly for businesses.

The European Union (hereinafter "E.U.") serves as an ideal model for the United States when it comes to a uniform system for data protection. The E.U. has recognized the growing importance of safeguarding the personal information of its citizens and created a cybersecurity regulation called the General Data Protection Regulation (hereinafter "GDPR"), which took effect in 2018.[19] The GDPR is one of the most comprehensive pieces of data protection legislation of our generation and is controversial during a time when mass data mining is a major resource for many businesses.[20] The GDPR lays out requirements and guidelines to businesses that are collecting personal data from its consumers. The GDPR requires compliance from E.U. businesses and extends to any business that serves E.U. citizens.[21] As with any substantial change in industry, the GDPR is not free of critics.

Some believe that GDPR compliance will be more complicated for smaller businesses, making them more susceptible to potential fines.[22] There is also a concern that free services that rely on data mining to function will cease to operate if they are unable to find new sources of revenue.[23] No matter the opinion on the GDPR, it is a regulation that is altering the way the U.S. is looking at data regulation. Colorado's Consumer Data Privacy Act[24] and California's Consumer Privacy Act[25] reflect the GDPR's influence.

---

[18] Petrina McDaniel, *Data Breach Laws on the Books in Every State; Federal Data Breach Law Hangs in the Balance,* SQUIRE PATTON BOGGS, (Apr. 30, 2018), https://www.securityprivacybytes.com/2018/04/data-breach-laws-on-the-books-in-every-state-federal-data-breach-law-hangs-in-the-balance/.

[19] *General Data Protection Regulation (GDPR),* GDPR.EU, https://gdpr.eu/tag/gdpr/ (last visited May 2, 2020).

[20] Espen Berg-Larsen, *The Issue of Privacy in the European Union: Controversies of the General Data Protection Regulation,* UNIV. OF OSLO (2015), http://urn.nb.no/URN:NBN:no-52422.

[21] *Fines and Penalties,* GDPR-INFO.EU, https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(4)%20GDPR%20sets%20forth,to%20that%20used%20in%20Art. (last visited Jun. 29, 2020).

[22] Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#2757190f94ad.

[23] *Id.*

[24] HB 18-1128, 71st Gen. Assemb., Reg. Sess. (Colo. 2018) (enacted).

[25] CAL. CIV. CODE § 1798 (2018).

In 2018, Colorado passed the Colorado Consumer Data Privacy Act (hereinafter "CDPA"), which requires that any business using Colorado citizens' data take "reasonable security measures" to protect that information.[26] The statute also requires the business to have a written policy for maintaining and destroying the data, along with complying with specific protocols in the event of a data breach.[27]

The California Consumer Privacy Act (hereinafter "CCPA") took effect in January 2020.[28] The CCPA will have reach beyond the borders of California because the state has the fifth-largest economy in the world.[29] The CCPA, much like the CDPA, requires any business that collects personal information[30] about California residents to implement "reasonable security" measures to protect their data.[31] Further, the statute creates a private right of action against a company that fails to employ reasonable security measures in protecting citizens' data.[32] The CCPA and the GDPR share the goal of providing autonomy and transparency to its citizens concerning the collection, use, and storage of their personal data.

This Note will provide a brief overview of the GDPR, while also discussing the practical advantages and disadvantages of adopting a similar regulation in the U.S. While U.S. businesses are subject to GDPR when serving E.U. citizens, U.S. companies are under no

---

[26] Jenifer McIntosh, *Privacy Basics for Colorado Lawyers: The Colorado Consumer Data Privacy Act and the California Consumer Privacy Act*, COLO. LAW., August/September 2019, at 26, 28.

[27] *Id.*

[28] Mike Gillespie, *Why Europe's GDPR Privacy Regulation is Good For Business,* COMPUTERWEEKLY.COM (Nov. 10, 2017), https://www.computerweekly.com/opinion/Why-Europes-GDPR-privacy-regulation-is-good-for-business.

[29] Matthew A. Winkler, *California Must Be Doing Something Right in Trump's America*, BLOOMBERG (May 29, 2018, 10:00 AM EDT), www.bloomberg.com/opinion/articles/2018-05-29/trump-vs-california-state-s-economy-vastly-outpaces-u-s.

[30] Personal information is not limited to personal data entered by the resident. McIntosh, *supra* note 26, at 27. Personal information also includes inferences that can be drawn from personal information – such as preferences, behavior, and intelligence. *Id.*

[31] Practical Law Data Privacy Advisor, *Understanding the California Consumer Privacy Act (CCPA)*, PRACTICAL LAW, https://1.next.westlaw.com/Document/I2b247b29e10b11e8a5b3e3d9e23d7429/View/FullText.html?originationContext=document&transitionType=DocumentItem&contextData=(sc.Folder*cid.4ccbc0c178e745e6b86a0dab2c98c200*oc.DocLink)#co_anchor_a208782 (last visited June 16, 2020); *see also* CAL. CIV. CODE § 1798.81.5(a). "The CCPA does not define reasonable security and it is not codified elsewhere in California law. However, other California statutes similarly require that businesses that own, license, or maintain personal information about California residents provide reasonable security for that information." *Id.*

[32] *Id.*

similar federal obligations when dealing with American citizens. The GDPR is a useful model for the U.S. to utilize. It has a global effect in countries where the legislation does not even reach, as evidenced by CCPA and the like. The states are beginning to advance new data privacy legislation, and cases concerning conflicting data privacy laws may soon come before the courts.

To provide this analysis, section II will begin by examining the growing industry of data analytics. Section III will provide a general discussion of the GDPR and the Articles that are relevant to this Note. Section IV will analyze the relationship between the GDPR and U.S. businesses. Section V will delve into current federal laws in the U.S. that relate to data privacy. These federal laws regulate certain industries and do not have a broad application. Section VI will consider Colorado's recently enacted Consumer Data Privacy Act, and California's Consumer Privacy Act. Section VII will discuss the U.S. adopting the GDPR as a model for data privacy legislation. Finally, Section VIII will conclude by summarizing the arguments in this Note for adopting the GDPR as a model for federal data breach legislation.

II. THE GROWING INDUSTRY OF DATA ANALYTICS

Data analytics has always existed in one form or another. However, in the digital age, data analytics has rapidly evolved to become a driving force behind marketing and sales techniques.[33]

Data analytics is the science of analyzing raw data in order to make conclusions about that information.[34] Data analytics techniques can reveal trends and metrics that would otherwise be lost in the mass of information.[35] Businesses can use this information to optimize processes and increase the overall efficiency of a business or system.[36] These programs learn trends that may be useful to businesses. By learning about these trends in consumer activity, businesses can adapt to meet their ideal market.

In the digital age, personal data is likened to a natural resource, which, when tapped into appropriately, can provide a stream of

---

[33] *Id.*

[34] Jake Frankenfield, *Data Analytics*, INVESTOPEDIA, https://www.investopedia.com/terms/d/data-analytics.asp (last updated Apr 27, 2019).

[35] *Id.*

[36] *Id.*

valuable information to a business.[37] Marketing and advertising agencies use personal data to inform businesses on tactics such as targeted advertising.[38] Data collection, or data mining, is not limited to marketing and advertisement agencies. Businesses often purchase collected information, i.e., data from a particular group of consumers, and use that information to inform its business model.[39] Some companies, such as Google, monitor and sell users' data to third parties.[40] Free services, such as Google, Facebook, and YouTube, are able to operate because they make money by selling users' data.

Data analytics and mass data mining go hand-in-hand. By collecting and analyzing personal data from consumers in mass quantities, businesses can more effectively learn about an individual's behavior.[41] Data processing has evolved through the use of Artificial Intelligence (hereinafter "AI") as a more efficient means of extracting useful information from an individual's personal data.[42] AI means that larger quantities of data can be processed faster.[43] As the use of AI continues to grow in businesses, it will increase the value of personal data.

Data analytics has the potential to provide useful information about consumers to businesses. Yet, data collected by mass data mining is not always the most reliable or helpful information. In fact, a significant amount of stored data is fruitless.[44] While organizations continue to collect mass quantities of data, only a fraction of that data has long-term utility.[45] A study conducted by Veritas Technologies in

---

[37] Matsakis, s*upra* note 1.

[38] Max Eddy, *How Companies Turn Your Data Into Money,* PCMAG (Oct. 10, 2018), https://www.pcmag.com/news/how-companies-turn-your-data-into-money.

[39] *Id.*

[40] *Id.*

[41] For example, learning the shopping habits of a consumer or a particular consumer can help companies to tailor advertising during certain times of the day. By knowing when a consumer is more likely to scroll through a clothing catalog, businesses can determine which marketing time slots are more beneficial.

[42] Sandra Wachter & Brent Mittelstadt*, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494, 500 (2019).

[43] AI can process data at an expediated rate compared to a human. From the data that is given, it draws predictions about behaviors, preferences, and private lives of individuals.

[44] *Veritas Global Databerg Report Finds 85% of Stored Data is Either Dark or Redundant, Obsolete, or Trivial,* VERITAS (March 15, 2016), https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data [hereinafter VERITAS].

[45] *Id.*

2016 found that approximately 85% of stored and processed data by organizations around the world is either dark,[46] redundant, obsolete, or trivial.[47] This means that a majority of the data which businesses are storing is completely useless to them. Although this data may be useless to a company, it can increase the risk for a consumer in the event of a data breach. If a company is storing redundant or duplicative data from a consumer, there is now a higher risk that the data can be compromised.

This data is being held either on a business's physical servers or on remote servers, typically through "cloud" technology.[48] The growth in the use of cloud-based storage makes it easy to store information remotely. As evidenced by the percentage previously mentioned, quantity has the potential to overtake quality. The use of cloud technology to remotely store information has enabled a data hoarding culture. Additionally, the mass amounts of unused data are now vulnerable to hackers.

Businesses making use of data analytics should be responsible for the storage and use of their data. In the first half of 2018, a comprehensive analysis of security breaches showed over three billion records were compromised due to data breaches.[49] These records were compromised during the nine-hundred-and-forty-four reported breach incidents in 2018.[50] Though many state laws create notification requirements in the event of a breach,[51] most lack regulations that create an obligation to store consumer data safely.

Organizations that utilize data analytics owe a duty to keep that information safe. Businesses rely on personal data as a driving force for their day-to-day decision-making. This personal data provides an insight into the consumer and is extremely valuable in the digital age. The increased value and reliability of personal data have caused a cultural shift, and individuals deserve basic information as to how their personal data is being used and processed.

---

[46] Dark data is data whose value is unknown.

[47] VERITAS, *supra* note 44.

[48] For example, most of a user's data on an iPhone is backed up to a remote server called iCloud.

[49] Breach Level Index, *supra* note 11.

[50] *Id.*

[51] Digital Guardian, *The Definitive Guide to US State Data Breach Law,* https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf (last visited Oct. 13, 2019).

Governments are responsible for protecting individuals from having their personal data used without their knowledge. Progressive lawmakers in the European Union recognize the importance of individual autonomy over personal data and have taken a significant step in delivering that autonomy by implementing the GDPR. The GDPR puts the privacy interests of individuals back into their hands. Some state lawmakers have acknowledged their responsibility to protect their citizens personal data and have passed legislation to that effect. This isn't the case in every state. In order to provide uniformity, the U.S. should follow the E.U.'s lead by implementing federal legislation similar to the GDPR.

III. GDPR AT A GLANCE

The E.U. established the GDPR to protect European citizens from mass data mining and data breaches by providing strict guidelines for organizations operating within the E.U. The GDPR applies to personal data, which includes any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to a personal identifier.[52] For a business to determine what data is personal data, "the content, purpose or result of the data processing must relate to an identifiable person either directly or indirectly."[53] In other words, personal data is information gathered that can be linked to an individual. These guidelines restrict organizations from mass data mining and grant citizens a legal right to know when and how companies use their personal information.[54]

The GDPR applies to organizations within the E.U. as well as organizations outside of the E.U. that offer goods or services to, or monitor the behavior of, European citizens.[55] Even if an organization is not solely serving E.U. citizens, it might be easier for that organization to comply with the heightened standard set by the GDPR in lieu of having different privacy standards for different consumer

---

[52] *FAQ*, GDPR.EU, https://gdpr.eu/faq/ (last visited May 3, 2020).

[53] Wachter & Mittelstadt, *supra* note 42, at 517.

[54] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 13-14, 2016 O.J. (L 119) 40-42 (EU) [hereinafter GDPR].

[55] *FAQ*, *supra* note 52.

bases. In this way, the GDPR is conceivably setting a de facto global standard.[56]

Under the GDPR, "controllers" and "processors" are required to satisfy particular standards. Article 4 of the GDPR defines a "controller" as the "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"; a "processor" is the "natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller."[57] The GDPR generally treats the data controller as the principal party for responsibilities such as collecting consent, managing consent revocation, and enabling rights of access to personal data.[58] For example, if ABC company sells widgets and uses the DEF company to track its consumers' engagement activity, then ABC company is the data controller, and the DEF company is the data processor.

The GDPR is enforced by data protection officers who work for supervisory authorities.[59] Each member state in the E.U. has its own separate supervisory authority responsible for a given jurisdiction. If a data breach involving personally identifiable information of E.U. citizens occurs, the organization must report the breach to the appropriate supervisory authority within seventy-two hours.[60] The supervisory authority, through the data protection officer, has the power to investigate the breach and obtain any information necessary to perform the investigation.[61]

A. Articles

This section will focus on the interplay among Articles Thirteen, Fourteen, Fifteen, Seventeen, and Twenty-Two. These sections of the GDPR create notice and access rights to individuals whose personal data is being collected by organizations. By giving

---

[56] Samantha Cutler, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect Eu Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1520 (2018).

[57] GDPR, *supra* note 54, art. 4(7)-(8), at 33.

[58] *What are 'Controllers' and Processors'?*, INFO. COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/ (last visited May 18, 2020).

[59] GDPR, *supra* note 54, art. 31, at 56.

[60] *Id.* art. 33, at 52.

[61] *Id.* art. 58, at 69.

citizens power over their personal data, the GDPR provides transparency to E.U. citizens while simultaneously increasing the accountability of organizations that collect and process personal data.[62]

Controllers must provide a lawful basis to the consumer for the data they have collected and the data processing they are engaging in.[63] This provides clarity to the consumer and forces businesses to take inventory of the data they already have and for what they are using it. This requirement is helpful to businesses by obligating them to create a plan for the data being collected, therefore optimizing their time and resources. Data controllers may also be required to provide this information to a supervisory authority if they are under investigation.[64]

Articles Thirteen and Fourteen convey transparency rights to citizens by requiring notification to an individual whose personal data has been obtained either through that organization directly or through a third party.[65] When the organization collects data, it must provide the individual with information about how the organization will process the data and information about potential third-party recipients of that data.[66] Further, the individual must be notified of her right to request access to, rectify any issues with, or delete her data from the controllers' database.[67]

The organization must stay within the original scope of consent obtained from the consumer. If the organization wants to use an individual's data for other purposes, it must request additional consent.[68]

Articles Thirteen and Fourteen contain almost identical provisions. The former addresses controllers, and the latter addresses processors.[69] Article Fifteen empowers the individual with a right of access to the personal data being collected and processed.[70] The

---

[62] Stefan Ducich & Jordan L. Fischer, *The General Data Protection Regulation: What U.S.-Based Companies Need to Know*, 74 BUS. LAW. 205, 209 (2019).

[63] Lesley E. Weaver & Anne K. Davis, *The Interplay of the European Union's General Data Protection Regulation and U.S. E-Discovery — One Year Later, the View Remains the Same*, 29 NO. 1 COMPETITION: J. ANTI., UCL & PRIVACY SEC. CAL. L. ASSOC. 159, 161 (2019).

[64] GDPR, *supra* note 54.

[65] Wachter & Mittelstadt, *supra* note 42, at 543.

[66] GDPR, *supra* note 54, art. 13, at 40-41; *id.* art. 14, at 41-42; *id.* art. 15, at 43; *id.* art 22, at 46.

[67] *Id.* art. 13(2), at 41; *id.* art. 14(2), at 42; *id.* art. 15(1), at 43.

[68] *Id.* art. 13(3), at 41

[69] *Id.* art. 13, at 40-41; *id.* art. 14, at 41-42.

[70] *Id.* art. 15, at 43.

controller is "obligated to provide a copy of the personal data undergoing processing."[71] When gaining the consent of individual users, the provisions require the organization to articulate the purpose of the data clearly.

These requirements are a significant step forward for individual autonomy in the digital landscape. These requirements will pressure businesses to ensure that they have a clear vision of what they are doing with collected data. These provisions put citizens in the driver's seat when it comes to the use of their personal data—if they so choose.

Article Fifteen does not inhibit the creativity or flexibility in the way an organization conducts its business; it simply requires that an organization provide a clear explanation of the goals the business wishes to reach with the data it is collecting.[72] This Article requires disclosure to a reasonable degree. Lawmakers were cognizant of the potential concerns of businesses when it came to weighing transparency and a competitive edge. Businesses are only required to disclose to the extent that it does not adversely impinge on sensitive internal information relating to the business.[73] For example, a consumer or data protection officer can ask a business to disclose what it plans to do with data, but the exact process may not be subject to disclosure if it is considered a trade secret.[74] Disclosure is to be determined by a data protection officer on a case-by-case basis.[75]

Under Article Seventeen of the GDPR, individuals have the right to have personal data erased.[76] This is also known as "the right to be forgotten."[77] This right attaches to a multitude of situations. Examples include the data subject's withdrawal of consent from processing,[78] or when personal data is no longer necessary for the purposes it was initially collected or processed.[79] A request for erasure extends to all known third-party data providers. Upon receiving that request, organizations must notify other businesses to erase the data

---

71 *Id.*
72 *Id.*
73 Wachter & Mittelstadt, *supra* note 42, at 546.
74 *Id.*
75 *Id.*
76 GDPR, *supra* note 54, art. 17, at 43-44.
77 Wachter & Mittelstadt, *supra* note 42, at 502.
78 GDPR, *supra* note 54, art. 17(1)(b), at 44.
79 *Id.* art. 17(1)(a), at 43.

they have received from the data subject.[80] If a company does not notify these parties, it risks being fined.

Article Twenty-Two regulates the use of AI to process data. This Article only applies when a decision is based *solely* on algorithmic decision-making and when the decision-making process produces "legal effects" or "similarly significant" effects on the individual.[81]

Ethical scholars are concerned that AI can lead to "privacy invasive and non-verifiable inferences that cannot be predicted, understood, or refuted."[82] Unlike a human assessor, AI cannot be questioned to determine bias. It is simply acting based the methodology it has been programmed to follow and the data it has processed. Seemingly, the E.U. recognized the potential ethical issues with AI and sought regulation through Article Twenty-Two of the GDPR. Article Twenty-Two provides E.U. citizens with the right to prevent their data from being subject to profiling as a result of a decision or inference made by automated processing, or AI.[83]

Through a process called "inferential analytics," AI is used to process large quantities of data and create a prediction based on an observed pattern.[84] If there is insufficient data to make a decision on a particular subject, AI can infer the rest of the information sought.[85] For example, inferential analytics can be used as assessors in health insurance companies to determine the risk involved in providing insurance to a certain person.[86] If the health insurance company relies on an algorithm to decide whether to provide an individual with insurance and, if so, what type to provide, there is a risk that the data on which the algorithm relies could hold learned biases.[87]

Further, this Article requires the controller to "implement suitable measures to safeguard the data subjects' rights and freedoms

---

[80] *Id.* art. 17(2), at 44.

[81] Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 197 (2019).

[82] Wachter & Mittelstadt, *supra* note 42, at 497.

[83] GDPR, *supra* note 54, art. 22, at 46.

[84] *Inferential Statistics*, DEEPAI.ORG, https://deepai.org/machine-learning-glossary-and-terms/inferential-statistics (last visited May 18, 2020).

[85] *Id.*

[86] Starre Vartan, *Racial Bias Found in a Major Health Care Risk Algorithm,* SCI. AM. (Oct. 24, 2019), https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/ .

[87] *Id.*

and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision."[88] At a glance, this Article is stepping into the process of automation and compelling a portion of human involvement.

There are three exceptions to the Article Twenty-Two requirement.[89] The first is when the automated decision is "necessary for a contract."[90] The second is when a Member State of the European Union has passed a law creating an exception.[91] The third is when an individual has explicitly consented to algorithmic decision-making.[92]

These safe harbors carve out some limited exceptions to Article Twenty-Two. Absent consent, the vagueness of the statute may pose issues for organizations and businesses which rely on the use of AI in their data processing systems.[93] Working party guidelines[94] clarify that Article Twenty-Two is a prohibition on algorithmic decision-making, not a mere right to object to it.[95] Companies that currently use and wish to continue using this type of decision-making must assess under which exception they fall.[96] Further, the guidelines explain that for an automated decision to fall outside of Article Twenty-Two, human involvement must be meaningful.[97] Human oversight must be carried out by someone who has the authority and competency to change the decision.[98] Organizations using and developing AI will have to exercise some creativity in ensuring compliance with the GDPR. AI does not program itself,[99] but with the growing use of automation, the GDPR aims to ensure a check on these systems.

---

[88] GDPR, *supra* note 54, art. 22(3), at 46.

[89] *Id*.

[90] *Id.*

[91] *Id.*

[92] *Id.*; *see also* Kaminski, *supra* note 81.

[93] Kaminski, *supra* note 81, at 201.

[94] The working party was an advisory board made up of a representative from the data protection authority of each EU Member state, the European Data Protection Supervisor, and the European Commission. As of May 25, 2018, it has been replaced by the European Data Protection Board. *National Data Protection Authorities*, European Commission: Justice and Consumers, EUROPA.EU (Sept. 21, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

[95] Kaminski, *supra* note 81, at 201.

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] That is, not typically.

Articles Thirteen and Fourteen arm citizens with knowledge about how companies use their personal data, which is essential to Article Fifteen's requirement of obtaining an individual's informed consent for the use of her data.[100] Arguably, this transparency can create tension for organizations that consider their manner of processing personal data essential to their business model.

One of the foreseeable drawbacks of the GDPR is that it may interfere with a business's competitive edge. More specifically, companies might consider the manner in which they process personal data as a trade secret. Being compelled to disclose that information impedes the commercial advantage a company would reap from a unique or innovative process. However, the E.U. has implemented broad protections for companies who fear that disclosure of their data processes would impede commercial advantages that flow from these processes.[101]

Big data is one of the fastest-growing businesses because data is such an invaluable resource to organizations that want insight into their consumers.[102] Companies from Amazon to Starbucks use big data in areas such as customer relations or determining where to open a new location.[103] Having this feedback is essential to a well-run business but should also come with a responsibility to keep that data safe.

The GDPR seeks to strike a balance between individual autonomy and the freedom to conduct business. Some organizations criticize the regulation as overbroad, while others argue the GDPR does not go far enough. [104] For example, in a survey conducted by the

---

Eddie Gent, *Artificial intelligence is evolving all by itself,* SCIENCEMAG.ORG (Apr.3, 2020), https://www.sciencemag.org/news/2020/04/artificial-intelligence-evolving-all-itself.

[100] GDPR, *supra* note 54, art. 15, at 43; *id.* art. 7, at 37.

[101] Kaminski, *supra* note 81, at 203.

[102] Research and Markets, *Big Data Analytics Industry Report 2020 – Rapidly Increasing Volume & Complexity of Data, Cloud-Computing Traffic, and Adoption of IoT & AI are Driving Growth*, GLOBENEWSWIRE (Mar. 2, 2020), https://www.globenewswire.com/news-release/2020/03/02/1993369/0/en/Big-Data-Analytics-Industry-Report-2020-Rapidly-Increasing-Volume-Complexity-of-Data-Cloud-Computing-Traffic-and-Adoption-of-IoT-AI-are-Driving-Growth.html; *see also IDC Forecasts Revenues for Big Data and Business Analytics Solutions will Reach $189.1 Billion This Year with Double-Digit Annual Growth Through 2022,* IDC (Apr. 4, 2019), https://www.idc.com/getdoc.jsp?containerId=prUS44998419.

[103] Eleanor O'Neill, *10 Companies That Are Using Big Data,* ICAS (Sept. 23, 2016), https://www.icas.com/thought-leadership/technology/10-companies-using-big-data.

[104] Roslyn Layton & Julian Mclendon, *The GDPR: What It Really Does and How the U.S. Can Chart A Better Course,* 19 FEDERALIST SOC'Y REV. 234, 245 (2018); *see also* Gavin

Chartered Governance Institute, some of those polled believed that the GDPR has become a "huge burden on resources" and created "much extra work for little extra benefit."[105] However, in that same survey, thirty-nine percent of those polled said that the GDPR has "significantly" improved their understanding of data protection.[106] Some scholars suggest the GDPR be taken a step further by providing guidelines for data evaluation as well as data collection.[107] Whether businesses agree with the regulation or not, hefty fines associated with non-compliance ensure that companies take the GDPR seriously.

B. Fines

The determination of fines is administered by individual member state supervisory authorities. The fines and penalties are determined by criteria such as the nature of the infringement, intent, mitigation of damages to data subjects, preventative measures taken, history of data security, cooperation with the investigation, and the type of data being collected.[108] The floor for these penalties is up to ten-million-euros (just over eleven-million USD), or two-percent of the worldwide annual revenue of the prior financial year, whichever is higher.[109] The ceiling is up to twenty-million-euros, or four percent of the worldwide annual revenue of the prior financial year, whichever is higher.[110]

In 2018, Facebook admitted that it had discovered a bug in its security program that allowed hackers to access the information of roughly fifty-million accounts.[111] This single data breach left Facebook facing a fine of up to one-billion-six-hundred-million-

---

Hinks, *GDPR: Data Protection Rules Seen as 'Burdensome' One Year on*, BOARD AGENDA (July 30, 2019), https://boardagenda.com/2019/07/30/gdpr-data-protection-rules-seen-as-burdensome-one-year-on/; Dennis Dayman, *Stop Whining, GDPR is Actually Good for Your Business,* THENEXTWEB.COM (Mar. 18, 2018), https://thenextweb.com/contributors/2018/03/18/stop-whining-gdpr-actually-good-business/.

[105] Hinks, *supra* note 104.

[106] *Id.*

[107] Wachter & Mittelstadt, *supra* note 42, at 615-16.

[108] *Fines and Penalties*, *supra* note 21.

[109] *Id.*

[110] *Id.*

[111] Arjun Kharpal, *Facebook Could Face up to 1.6 billion in Fines over Data Breach as Regulators Eye Formal Probe*, CNBC, https://www.cnbc.com/2018/10/02/facebook-data-breach-social-network-could-face-eu-fine.html (last updated Oct. 3, 2018, 4:04 AM EDT).

dollars.[112] Fines of this magnitude serve as an incentive for European and American businesses, that offer services to E.U. citizens, to become GDPR compliant.

The costs associated with violations of the GDPR are meant to compel businesses further to create a structure for the collection and use of personal data.[113] One of the criticisms of the GDPR is that the fines are excessive and burdensome to businesses.[114] However, there are alternatives to these fines. If a regulator deems a business to be non-compliant, the regulator also has the option to issue a corrective order to the business, allowing it a period of time to try and resolve the issue.[115]

IV. GDPR AND THE U.S.

The GDPR provides increased autonomy to E.U. citizens by requiring organizations to be transparent about how their data is collected, used, and processed. The GDPR applies to businesses operating within the E.U. and any businesses that utilize E.U. citizens' personal data.[116]

This regulation reaches across the pond to U.S. businesses. The E.U. and the U.S. have the largest bilateral trade and investment relationship and enjoy the most integrated economic relationship in the world.[117] This transatlantic relationship also defines the shape of the global economy as a whole. Either the E.U. or the U.S. is the largest trade and investment partner for almost all other countries in the global economy.[118] The E.U. and U.S. economies combined account for about half the entire world GDP and nearly a third of world trade flows.[119] It is no wonder that with a trade relationship such as this, the

---

[112] *Id.*

[113] Ducich and Fischer, *supra* note 62, at 212.

[114] Bob Noel, *GDPR Compliance, the Supervisory Authority, and How Much Money a Fine Could Cost,* PLIXER (Feb. 27, 2018), https://www.plixer.com/blog/gdpr-compliance-supervisory-authority-much-money-fine-cost/.

[115] GDPR, *supra* note 54, art. 58(2), at 70.

[116] Max Read, *The E.U.'s New Privacy Laws Might Actually Create a Better Internet,* N.Y. MAGAZINE (May 15, 2018), https://nymag.com/intelligencer/2018/05/can-gdpr-create-a-better-internet.html.

[117] *Countries and Regions: United States*, EUROPEAN COMMISSION, https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (last updated Apr. 23, 2020).

[118] *Id.*

[119] *Id.*

GDPR has a significant effect on U.S. businesses. U.S. businesses may have to comply with the GDPR by default to continue doing business or provide services to E.U. citizens.[120] With the amount of economic interaction between the U.S. and the E.U., perhaps, the U.S. could stand to enforce the GDPR and its regulations. However, the enforcement of a foreign regulation would certainly raise some red flags on U.S. soil.

The GDPR is an E.U. regulation, and arguably it should be left to the E.U. to enforce it. At this point, the U.S. has not formally adopted the GDPR. Still, many businesses have self-regulated to ensure compliance with the regulation if they are doing business that falls under the scope of protection afforded under the GDPR.[121]

The E.U. has taken the bull by the horns when it comes to protecting its citizens' personal data. The regulation creates a set of uniform guidelines for businesses to follow. The E.U. regulations are distinguishable from those in the U.S. in many ways. One of them is evident through the GDPR. The requirements in the GDPR apply as soon as consumer data is being collected. In contrast, many American regulations typically provide guidelines for businesses to follow once a data breach has already occurred. U.S. lawmakers stand to learn from the proactive, instead of reactive, nature of the GDPR.

Many states are grappling with the issue of data protection.[122] A majority of data privacy laws that exist in the U.S. provide notification requirements in the event of a breach.[123] These types of laws ignore the larger issue at hand, sloppy mass data mining.

In many states, the law allows companies to withhold notice of a breach from individuals unless they determine there is a "substantial risk of harm."[124] This means that the company responsible for the

---

[120] Chris Bennington, *U.S. Hospitals Will Continue to Grapple with GDPR Compliance in 2019,* JDSUPRA (Jan. 10, 2019), https://www.jdsupra.com/legalnews/u-s-hospitals-will-continue-to-grapple-22526/.

[121] *GDPR for US Companies,* COMPLIANCE JUNCTION, https://www.compliancejunction.com/gdpr-for-us-companies/ (last visited May 3, 2020); *see also* Rakesh Soni, *Are you Ready for America's Data Protection Laws?*, VENTUREBEAT (Oct. 12, 2019), https://venturebeat.com/2019/10/12/are-you-ready-for-americas-data-protection-laws/.

[122] Kyle Schryver, *The Future of Data Privacy in the United States,* CPO MAGAZINE (Aug. 1, 2019), https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-in-the-united-states/.

[123] Digital Guardian, *supra* note 51.

[124] ALA. CODE § 8-38-5 (2018); *see also* ALASKA STAT. § 45.48.010 (2009); ARK. CODE § 4-110-105(d) (2019); CONN. GEN. STAT. § 36a-701b(b) (2018); DEL. CODE ANN. tit. 6, § 12B-102(a) (West 2018); HAW. REV. STAT. § 487N-1 (2008); LA. STAT. ANN. § 51:3074(I) (2018);

breach is now in charge of determining whether to notify the individuals affected. Other states do not require notice absent a reasonable likelihood to cause "substantial economic loss to an individual."[125] As a further example, Indiana laws require notification to a consumer only when the business that suffered the breach can reasonably foresee the breach resulting in identity theft, fraud, or identity deception.[126] These laws provide a glimpse into the fractured nature of American data privacy and security laws. It also highlights the need for a uniform body of law.

State legislatures cannot reliably determine whether there is a "reasonable likelihood of misuse" without an understanding of the contours of data privacy and legislation. These laws also exemplify tension that exists between U.S. businesses' interest in self-regulation and the legislature's ability to hold those businesses accountable for harm done to its citizens. Unfortunately, under these risk assessments, it is often the most interested party—the company—that assesses whether there is such a harm.

It is imperative for lawmakers to focus on more than the cleanup stage that breach notification regulations address. Providing a baseline for businesses to follow at the outset of data collection could potentially prevent future data breaches. Compelling businesses to pay attention to and safeguard the data they rely on not only protects citizens' data but, in the event of a breach, also saves those businesses money in the long run. According to Cisco's 2019 Data Privacy Benchmark Study, organizations that are GDPR compliant are less likely to have experienced a breach in the last year, and those that did suffer breaches lost fewer records and therefore saw smaller incident costs.[127]

OR. REV. STAT. § 646A.604(8) (2020); WASH. REV. CODE. §§ 19.255.010(1), 42.56.590(1) (2020);

[125] ARIZ. REV. STAT. ANN. § 18-551(10) (2018); *see also* FLA. STAT. § 501.171(4)(c) (2019); IOWA CODE. § 715C.2(6) (2018).

[126] IND. CODE § 24-4.9-3-1(a) (2020); *see also* KY. REV. STAT. ANN. § 365.732(1)(a) (West 2014); MASS. GEN. LAWS. ch. 93H, §§ 1(a), 3(b) (2007); MICH. COMP. LAWS § 445.72(3) (2011); Mo. Rev. Stat. § 407.1500(2)(5) (2018); N.M. STAT. ANN. § 57-12C-6(B) (2017); N.C. GEN. STAT. §§ 75-65(a) (2009), 75-62(14) (2016); UTAH CODE ANN. § 13-44-202(1)(b) (West 2019); W. VA. CODE § 46A-2A-102(a-b) (2020); WIS. STAT. § 134.98 (2)(cm)(1) (2019). Not all states are included in the footnotes because they either do not fall within the three standards, or do not have any risk assessment requirement.

[127] Dan Swinhoe, *Does GDPR Compliance Reduce Breach Risk?*, CSO ONLINE, https://www.csoonline.com/article/3369461/does-gdpr-compliance-reduce-breach-risk.html (Mar. 29, 2019).

The E.U. is taking an active role in protecting its citizens' data through the GDPR. The GDPR gives citizens the right to allow businesses to continue to use their data, while also empowering individuals to understand how companies are using their data. Armed with that information, individuals can decide for themselves whether they want to allow companies to use their personal data. This model is beneficial to businesses and consumers. The GDPR shows that lawmakers in the E.U. have an awareness and basic understanding of the value of personal data. Thus, Congress should follow the E.U. model in drafting and implementing its own set of federal data safety regulations.

V. CURRENT FEDERAL LAWS APPLICABLE TO DATA SECURITY

The U.S. needs a uniform network of laws that regulates personal data. Currently, there exists a medley of laws from different federal agencies that bear upon personal data and data security. The following federal laws provide regulation and guidelines for data privacy and security for certain industries, but that is not their main focus.[128]

A. FTC Act

The Federal Trade Commission (hereinafter "FTC") aims to protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices without unduly burdening legitimate business activity.[129] The FTC primarily regulates the protection of consumers' personal data under the umbrella of the FTC Act, which prohibits unfair or deceptive commercial practices.[130] The FTC has brought enforcement actions against companies for failing to protect consumers' personal data, leaving data vulnerable to cyberattacks, changing their privacy policies without adequate notice, and failing to comply with posted privacy policies.[131]

The FTC Act does not impose specific requirements on businesses, but does provide guidelines for what the FTC considers to

[128] This is not an exhaustive list.

[129] *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Feb. 18, 2020).

[130] 15 U.S.C. § 45(a)(1) (2020).

[131] Sloane, *supra* note 15, at 26.

be "best practices."[132] For example, the FTC does not require companies to maintain a privacy policy, but when a company discloses a privacy policy, the FTC requires that the company comply with the terms of that policy.[133]

The FTC Act does not address acquiring consent to use an individual's personal data. However, similar to the GDPR, it does suggest that organizations that revise their privacy policies should obtain additional consumer consent before using their data in ways that are materially different from the policy that was in effect when the data was first collected.[134]

The FTC also has Behavior Advertising Principles (hereinafter "BAP"), that apply to online service providers that engage in behavioral advertising.[135] BAP suggest that website operators should obtain express consent before using sensitive consumer data such as financial data, data about children, health information, precise geographic location information, and social security numbers.[136] Compliance with BAP is voluntary. The FTC has brought enforcement actions alleging that a failure to take reasonable and appropriate steps to protect personal information is an unfair act or practice.[137]

The FTC has determined that inadequate data security can form the basis for a deceptive practices claim. This was the heart of the issue in *F.T.C. v. Wyndham Worldwide Corp.*[138]

The FTC filed a complaint against Wyndham Worldwide Corp., claiming its failure to implement reasonable and appropriate security measures exposed consumers personal information that is likely to cause substantial consumer injury, including financial injury, to consumers and businesses.[139] In response to this complaint, the defendants in *Wyndham* moved to dismiss and challenged the FTC's

---

[132] *Id.* at 25.

[133] Leuan Jolly, *US Privacy and Data Security Law: Overview,* PRACTICAL LAW, https://1.next.westlaw.com/6-501-4555?isplcus=true&transitionType=Default&contextData=%28sc.Default%29 (last visited May 11, 2020).

[134] *Id.*

[135] *Id.*

[136] Sloane, *supra* note 15, at 27.

[137] In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467 (2005).

[138] 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[139] *See* Complaint, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

authority to bring data security actions.[140] Wyndham asserted that "generally, agencies cannot rely on enforcement actions to make new rules and concurrently hold a party liable for violating a new law."[141] Further, the defendant argued that the FTC "can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires – and the FTC has not done so here."[142] The FTC argued that "data security standards can be enforced in an industry-specific, case-by-case manner and that it has the discretion to enforce the FTC Act's prohibition of unfair practices through individual enforcement action rather than rulemaking."[143] Additionally, the FTC argued that fair notice does not necessarily require issuing regulations and that the FTC could never protect consumers from unfair practices if it first had to issue a regulation governing the specific practice at issue.[144] The district court ultimately denied Wyndham's challenge to the FTC's authority and ruled that the FTC need not issue regulations before bringing enforcement actions.[145] However, the court made it a point to conclude that this decision "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked."[146]

In the end, the parties reached a settlement agreement in which Wyndham agreed to implement and maintain a comprehensive data security program, obtain annual assessments of the security program, and provide copies of those assessments to the FTC.[147]

In another complaint filed by the FTC, it alleged that LabMD engaged in unfair trade practices by failing to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data.[148] LabMD filed a motion to dismiss.[149] Similar to the argument in *Wyndham,* the motion alleged that the FTC had no authority to address private companies' data security practices as

---

[140] *Wyndham*, 10 F. Supp. 3d 602, 616.

[141] *Id.*

[142] *Id.*

[143] *Id.* at 617.

[144] *Id.*

[145] *Id.* at 621.

[146] *Id.* at 610.

[147] Stipulated Order for Injunction at 4-5, F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 2:13-CV-01887-ES-JAD).

[148] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1225 (11th Cir. 2018).

[149] LabMD, Inc. v. Fed. Trade Comm'n, 776 F.3d 1275 (11th Cir. 2015).

unfair acts or practices.[150] The motion further alleged that the FTC violated LabMD's due process rights by failing to give fair notice of what security practices section 5 of the FTC Act forbids.[151] The court denied the motion. LabMD sought relief in the federal court, but the court dismissed LabMD's claims as premature because it had not yet exhausted its administrative agency remedies by obtaining a final FTC action.[152]

The complaint started at the administrative level, and, in November 2015, the administrative law judge dismissed the complaint because the FTC failed to prove that LabMD's data security practices caused or were likely to cause substantial consumer injury.[153] Then, in July 2016, the commissioners who heard the appeal reversed, concluding that the Administrative Law Judge who dismissed the complaint applied the wrong legal standard and found that LabMD's security practices either caused or were the likely cause of substantial consumer injury and that LabMD's data security practices were unreasonable.[154]

However, in June 2018, the Eleventh Circuit vacated the FTC's order because it "commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[155] Clearly, this ruling demonstrates the need for the FTC to provide more specific conditions to put businesses on notice of what it means to safeguard consumer data properly.[156] Further, another significant holding in this opinion is that FTC enforcement actions for unfair practices cannot be based solely on consumer injury. There must be a showing by the FTC that the unfair practice at the heart of its enforcement action was unconstitutional or violative of a specific statute or common law principle.[157] Now, the FTC faces a new

---

150 *Id.*

151 *Id.*

152 *Id.* at 1280.

153 In re LabMD, Inc., No. 9357, 2015 WL 7575033 at 2 (F.T.C. Nov. 13, 2015).

154 In re LabMD, Inc., No. 9357, 2016 WL 4128215 (F.T.C. Jul. 28, 2016).

155 LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236 (11th Cir. 2018).

156 Alison Frankel, *There's a Big Problem for the FTC Lurking in 11th Circuit's LabMD Data-Security Ruling,* REUTERS (Jun. 7, 2018, 4:26 PM), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

157 *Id.*

obstacle in cases where there is no specific statute or common law principle on which to rely.[158]

Having a comprehensive set of regulations would provide clarity to businesses and would legitimize the agencies that enforce the regulations. It would benefit agencies such as the FTC by providing the contours for specific causes of action, as well as putting applicable businesses on notice. The LabMD litigation started from a data breach that occurred in 2005 and did not come to an end until the summer of 2018.[159] If there were a standard set by the FTC, LabMD could have used its time, money, and other resources more efficiently. Comprehensive reform and robust data security legislation will also benefit the consumer by providing transparency about the protection and use of their personal information.

The FTC is the most involved administrative agency respecting consumer privacy rights and legislation.[160] However, the protections afforded by the FTC are inadequate and incomplete. The current policies of the FTC do not clearly lay out requirements for businesses—leading to an ambiguity that compromises an individual's personal information. Federal lawmakers must address data security and protection through clear and specialized legislation; it is not enough for it to fall under the category of "unfair or deceptive" practices broadly. A specialized piece of legislation would give express authority to agencies for enforcement and would also provide clear guidelines for businesses to follow.

B. The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (hereinafter "GLB")[161] is federal legislation that regulates the collection, use, protection, and disclosure of nonpublic personal information (hereinafter "NPI") by financial institutions.[162] In addition to financial institutions,[163] the GLB applies to third parties that receive NPI from financial institutions.[164] The GLB protects the NPI of consumers and customers.

---

158 *Id.*

159 *LabMD, Inc.,* 894 F.3d at 1224.

160 Sloane, *supra* note 15, at 25.

161 Also known as the Financial Services Modernization Act.

162 15 U.S.C. §§ 6801-09 (2011).

163 Companies that offer consumers financial products or services such as loans, financial or investment advice or insurance.

164 15 U.S.C. § 6802.

A consumer is someone who has obtained a financial product or service but does not have an ongoing relationship with the financial institution.[165] A customer is a subset of consumers who have an ongoing business relationship with an institution.[166] The GLB maintains notice and disclosure requirements for both customers and consumers.[167] However, the timing and content of the notice vary on whether the subject of the data is a consumer or a customer.[168] For example, a financial institution must provide notice of its privacy practices to a customer both at the outset of the relationship and annually.[169] However, for a consumer, the financial institution only needs to provide notice of its privacy practices if it intends to share the consumer's NPI.[170]

In either case, once triggered, the privacy practices disclosed by a financial institution must describe the categories of information that the financial institution collects and distributes, identify the categories of affiliated[171] and non-affiliated entities with which it shares information, state that the consumer or customer has the right to opt-out of some disclosures, and explain how the consumer or customer can opt-out if an opt-out right is available.[172] If the financial institution provides notice to the consumer of its practice of sharing NPI with an affiliated entity, it need not obtain consent from the consumer for the disclosure.[173] This provides a basic level of transparency to consumers and customers who fit within the criteria imposed by the GLB. There are carve-outs for this disclosure requirement that apply to compliance or law enforcement purposes.[174] The GLB does not require any affirmative consent from a customer or consumer.

The GLB requires financial institutions to explain their information-sharing practices "to their customers and to safeguard

---

165 Sloane, *supra* note 15, at 30-31.

166 *Id.* at 31.

167 15 U.S.C. § 6803.

168 Sloane, *supra* note 15, at 30-31.

169 *Id.*

170 *Id.*

171 An affiliated entity is any company that controls, is controlled by, or is under common control with another company and includes both financial and non-financial institutions.

172 Sloane, *supra* note 15, at 30-31.

173 *Id.*

174 *Id.*

sensitive data."[175] The GLB safeguards rule requires companies to develop a written information security program that describes how they protect customer information.[176] The security measures enforced by each company must be appropriate to the company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the consumer information the company handles.[177] As part of its program, each company must designate at least one employee to coordinate its information security program, identify and assess the risks to consumer information in each relevant area of the company's operation while evaluating the effectiveness of the current safeguards, select service providers that can maintain appropriate safeguards, contractually require service providers to maintain safeguards, oversee service providers handling of customer information, and evaluate and adjust the program in light of relevant circumstances.[178] Penalties for violation of the GLB vary on the authorizing statute of the agency that brings the enforcement actions.[179]

While the GLB requires financial institutions to explain their information-sharing practices, it is insufficient as a data protection policy. First, the GLB's safeguard requirements are not definitive and allow businesses to create illusory safeguard programs that may comply with the program requirements but do not truly safeguard data.[180] Having a definitive list of requirements for businesses would provide legislators with certainty that businesses are properly protecting personal information. It would also provide clarity to businesses that are required to comply with the GLB. Further, explicit requirements would provide predictability and reliability to consumers that, in the event of a data breach, there is a uniform system in place to hold companies accountable. Additionally, this would benefit businesses, allowing them to streamline and make more efficient their data protection practices.

---

[175] *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited May 11, 2020).

[176] Sloane, *supra* note 15, at 32.

[177] *Id.*

[178] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (April 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[179] Sloane, *supra* note 15, at 32.

[180] *Id.*

Another shortfall of the GLB is that it has limited application because it only applies to NPI collected by financial institutions.[181] This regulation simply does not go far enough. There needs to be data protection provided to all types of personal data, not just NPI. Businesses should be held responsible to protect all categories of personal data to which they are privy. Further, the GLB does not provide for any access rights for customers and also limits opt-out rights to specific instances. General access rights should be provided to consumers in order to provide procedures that allow those consumers to know which, when, and how businesses are using their data.[182]

C. HIPAA

The Health Insurance Portability and Accountability Act (hereinafter "HIPAA") regulates medical information and applies broadly to health care entities and their service providers.[183] Specifically, HIPAA governs individually identifiable health information.[184] The HIPAA Privacy Rule applies to the use, disclosure, collection, and maintenance of personal health information (hereinafter "PHI").[185] The HIPAA Security Rule provides standards for protecting PHI. The HIPAA Transactions Rule applies to some forms of electronic transmissions of health data.[186] These three rules provide guidelines for the proper procedures to protect individuals' PHI.

First, HIPAA requires, with some exceptions, that covered entities provide notice of their privacy practices and individuals' rights under HIPAA.[187] Second, an entity, which requires authorization to process a disclosure request, may only disclose the minimum amount

---

[181] *Id.* at 30.

[182] *Id.* at 34.

[183] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–91, 110 Stat. 1936; *see also Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, *HIPAA Privacy Rule*, CENTERS FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited May 18, 2020).

[184] *Id.*

[185] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited May 11, 2020).

[186] David C. Kibbe, *What the HIPAA Transactions and Code Set Standards Will Mean for Your Practice,* FAMILY PRACTICE MANAGEMENT, 28, 28-32, (Nov. – Dec. 2001) (discussing HIPAA transactions and code set standards).

[187] 45 C.F.R. § 164.520 (2013); 45 C.F.R. § 164.514 (2013).

of PHI necessary to complete a transaction.[188] Finally, the entity must implement data security procedures to protect PHI, ensure compliance with uniform standards for certain electronic transactions, and notify individuals if there is a security breach of PHI.[189]

HIPAA requires covered entities to provide notice of a PHI breach unless the covered entity demonstrates that there is a low probability that the data has been compromised.[190] This allows significant leeway for healthcare providers, although they may be subject to fines by the Department of Health and Human Services (hereinafter "HHS").[191] HIPAA's data protection regulations have a limited application, as they only apply to PHI. As with the previous regulations discussed, the most significant pitfall of HIPAA is its limited scope to only PHI. However, information not protected by HIPAA is just as valuable as PHI.[192]

Currently, Federal agencies do not provide clear and specific guidelines for data ptorection and deal with data security as a collateral issue. There is a need for a comprehensive set of rules that put companies on notice of what is required of them when it comes to protecting the personal information of its customers. The current regulations are laden with carve-outs, exceptions, and flexible standards that allow businesses to skirt around responsibilities. Some jurisdictions, such as California and Colorado, recognize this and have enacted data privacy regulations of their own.[193]

VI. RECENT PRIVACY LEGISLATION IN THE U.S.

The GDPR is a reminder that people lend their information to businesses, and those businesses have a responsibility to look after that information with care.[194] The trade relationship between the E.U. and the U.S. makes it nearly impossible for domestic businesses to ignore the GDPR. As a result of the GDPR's far-reaching influence, both

188 *Id.*

189 *Id.*

190 45 C.F.R. § 164.402 (2013).

191 *Id.*

192 Sloane, *supra* note 15, at 37.

193 HB 18-1128, 71st Gen. Assemb., Reg. Sess. (Colo. 2018) (enacted); CAL. CIV. CODE § 1798 (2020).

194 Gillespie, *supra* note 28.

California and Colorado have passed their own cybersecurity policies.[195]

A. Colorado Consumer Data Privacy Act

The CDPA was enacted in 2018 and is one of the first steps forward into more comprehensive cybersecurity policies in the U.S.[196] As with the GDPR, the CDPA applies to the personal data of businesses' clients.[197] More specifically, it applies to personally identifiable information.[198] However, the CDPA does not go as far as the GDPR.

The CDPA has three significant requirements for businesses in Colorado. First, the CDPA requires companies to take "reasonable security" measures to protect the information of their clients.[199] Second, the companies must have a written policy for maintaining and destroying the information collected.[200] Last, businesses must comply with protocols for assessing and reporting a data breach.[201] Companies must also ensure that any third-party service providers also comply with these regulations.[202]

In comparison to the GDPR, Colorado seems to be easing into the world of data security and regulation. However, one local newspaper calls this law "among the most demanding in the country."[203] The CDPA is a step in the right direction for Colorado and it applies to all businesses operating in Colorado, from mom-and-pop shops to large corporations.

B. California Consumer Privacy Act

In the spring of 2018, three news organizations published stories revealing that Cambridge Analytica had harvested the personal

---

195 *Supra* note 192.

196 McIntosh, *supra* note 26, at 26.

197 *Id.*

198 *Id.*

199 *Id.* at 28.

200 *Id.* at 26.

201 *Id.* at 28.

202 *Id.* at 27.

203 Joe Rubino, *Colorado's New Consumer Data Protection Law Among the Most Demanding in the Country*, THE DENVER POST (Sept. 4, 2018), https://www.denverpost.com/2018/09/04/colorado-businesses-consumer-data-protection-law/.

data of millions of people's Facebook profiles without their consent and for political purposes.[204] Following this jarring news, cybersecurity was at the forefront of the American public—this was especially true in California.[205] After the news broke, a group called "Californians for Consumer Privacy" worked on sweeping privacy legislation for presentation to California voters.[206] Later that summer, the CCPA was signed into law.[207] While the law is still a work in progress, evident by the many subsequent amendments, it is the first step toward a greater level of transparency and autonomy for California citizens when it comes to their personal information.

The CCPA serves to protect California consumer rights and encourage stronger privacy and greater transparency overall.[208] Under the CCPA, companies that use the personal information of California citizens must employ "reasonable security" measures to protect the data collected from California residents.[209] This legislation will have a significant effect on businesses throughout the U.S. because California has the fifth-largest economy in the world.[210] Under the California statute, an individual has a private cause of action if a business does not comply with the CCPA.[211]

In some ways, the CCPA is even more extensive than the GDPR. For example, the CCPA protects California citizens when it comes to their "personal information." Under the CCPA, "personal information" is not just information that directly identifies a person but also information that is "reasonably capable of being associated with

---

[204] Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Emma Graham-Harrison & Carole Cadwalladr, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[205] Dominique-Chantale Alepin, *Social Media, Right to Privacy and the California Consumer Privacy Act*, 29 NO 1. COMPETITION: J. ANTI., UCL & PRIVACY SEC. CAL. L. ASSOC. 96 (2019).

[206] *Id.*

[207] *Id.* at 97.

[208] Sloane, *supra* note 15, at 50.

[209] McIntosh, *supra* note 26, at 27.

[210] Kieran Corcoran, *California's Economy is Now the Biggest in the World, and Has Overtaken the United Kingdom,* BUSINESS INSIDER (May 5, 2018), https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5.

[211] Alepin, *supra* note 205, at 99.

or could reasonably linked to a particular consumer or household."[212] Thus, the CCPA protects data even if there is not a direct link to a person's identity. The threshold for determining whether a piece of data can be linked to a person is simply reasonableness.[213] The CCPA goes even further and applies protection to data which is reasonably linked to a specific household.[214] Currently, it is unclear whether the statute applies solely among family members or all occupants of a single dwelling.

The CCPA also creates affirmative obligations for businesses. First, it requires that businesses publish disclosures regarding their practices and consumers' rights with respect to the use of their personal data.[215] This is analogous to the GDPR's notification requirements in Articles Thirteen and Fourteen.[216] The CCPA also requires businesses to provide consumers with at least two methods to request information about their personal data.[217] Further, they must then comply with and respond to consumers' requests for information and provide that information in a usable format.[218] These requirements are similar to those in GDPR Article Fifteen.[219] The CCPA also requires businesses to allow consumers to opt-out of the sale of their personal information to third parties.[220] This section is strikingly similar to GDPR Article Seventeen's "right to be forgotten."[221] The CCPA is not a replica of the GDPR but has seemingly been inspired by the Articles mentioned earlier.

The CCPA is one of the first concrete examples of a state taking note of the GDPR and getting a leg up on data protection. California is making its mark as a trailblazer in the area of data protection and privacy. The CCPA is a significant evolution from the typical notification requirements in the multitude of data privacy statutes across the U.S.

---

[212] CAL. CIV. CODE § 1798.140(o)(1) (2020).

[213] *Id.* at § 1798.140(a).

[214] *Id.*

[215] CAL. CIV. CODE § 1798.100 (2019).

[216] Articles 13 and 14 require notification to an individual whose personal data has been obtained by an organization or by a third party.

[217] *Supra* note 212.

[218] *Id.*

[219] Article 15 empowers the individual with a right of access to the personal data being collected and processed.

[220] *Supra* note 212 at § 1798.140.

[221] GDPR, *supra* note 54, art. 17, at 43-44.

VII. DISCUSSION

As technology continues to evolve, and industries continue to grow on a global platform, the U.S. will inevitably have to regulate data privacy and protection on a federal level. As of 2019, cyber-attacks are considered among the top five risks to global stability.[222] Due to the lack of legislation in data protection, data breaches serve to threaten companies' revenues, and undermine consumer trust in those companies. The U.S. is a leader in the global economy, and American businesses rely on the use of personal data on a daily basis.[223] Even with data protection regulations in industries such as healthcare and finance, data breach statistics continue to rise.

Federal legislation is the best option to create uniformity and clarity throughout the U.S. in an area of the law that is not slowing down in the foreseeable future. While some states have implemented their own data protection legislation, others maintain data privacy standards that only create guidelines for businesses after a data breach has already occurred. In 2019, the average time to identify a breach was 206 days, while the average time to contain that breach was 73 days.[224] There is a need for a harmonization of data privacy policy to provide clear, preemptive regulations that protect consumers' personal data from the moment it is collected. Without proper federal intervention, the number of data breaches will only continue to grow.

The U.S. would not be the first global superpower to regulate data privacy. The E.U.'s GDPR is a successful model for the U.S. to follow. By providing proactive guidelines for businesses, the GDPR provides E.U. citizens with information and autonomy over their personal data, while simultaneously providing clarity to businesses for compliance. Despite critics claim that implementing a GDPR-equivalent regulation is too costly and burdensome on businesses[225], it has been proven that businesses who are GDPR compliant have saved money in the long run when dealing with costs that flow from a data breach.[226] Implementing a similar regulation stands to benefit both the consumer and the company.

---

[222] Sobers, *supra* note 13.
[223] *Id.*
[224] *Id.*
[225] Forbes, *supra* note 22.
[226] Swinhoe, *supra* note 127.

Additionally, safeguarding data through a harmonized federal regulation will reinforce consumer confidence with the businesses that are privy to their personal data. By setting a baseline that all companies must comply with, consumers can make informed decisions about the use of their personal data and rest assured that companies will be held accountable failure to safeguard personal data. Moreover, businesses will not have to parse through contradicting state laws to determine the best course for compliance. Uniformity in data protection laws will foster trust and efficiency between consumers and businesses, as well as companies that are in the business of exchanging personal data.

VIII. CONCLUSION

States like California and Colorado have already borrowed concepts from the GDPR in updating and enacting their own data privacy legislation. Other states have not updated their data security legislation in over ten years.[227] It will be interesting to see if other states follow California and Colorado's lead, or if California will create a de facto standard for data regulation policy in the U.S. in the same way the GDPR has become a de facto standard on a global scale.[228] California has the fifth-largest economy in the world[229] and has previously created regulations that became de facto nationwide guidelines. For example, California's emissions standards have fundamentally transformed the automobile industry in the U.S.[230]

In the digital age we live in, personal data is a valuable resource for businesses to capitalize on to learn about their consumers.[231] However, the quality of that personal information has quickly become overtaken by quantity. The GDPR combats this by forcing businesses to take stock of their collected data.[232] When consumers are granted access to their data and a legal right to question its use, businesses are compelled to comb through the data they have been sitting on and organize it so they can use it efficiently and effectively.

---

227 ALASKA STAT. § 45.48.010 (2009); *see also* HAW. REV. STAT. § 487N-1 (2008).

228 Cutler, *supra* note 56.

229 Winkler, *supra* note 29.

230 Russ Mitchell, *Automakers Vote for California in Emissions Debate,* GOVERNING (Nov. 27, 2019), https://www.governing.com/news/headlines/Automakers-Vote-for-California-in-Emissions-Debate.html.

231 Eddy, *supra* note 38.

232 GDPR, *supra* note 54, at 3.

By having an intimate knowledge of the data that they are collecting and what it is being used for, businesses should be able to prioritize and organize that data in a way that helps them run more resourcefully. Additionally, this reorganization and compliance with the GDPR have proved to help businesses avoid data breaches and lower costs in the event of a breach.[233]

Technology is evolving with each passing day and, if lawmakers do not start to pay attention now, they may become lost in the current. There needs to be an organized effort to protect the personal information of citizens, and it needs to happen now.

[233] Swinhoe, *supra* note 127.